это средства, как будут оценивать результаты работ, выполненных в рамках государственных заказов, не имея в штате соответствующих специалистов, пока совершенно неясно. Да и органы исполнительной власти, уполномоченные в области безопасности и технической защиты информации, такие документы по закону согласовывать вовсе не обязаны, в отличие, скажем, от предложений ассоциаций и союзов операторов персональных данных, пожелавших в дополнение к угрозам, установленным ФСБ, ФСТЭК и профильными ведомствами, добавить свои, про которые вышестоящие органы не знают. Для таких случаев порядок согласования установлен специальным Постановлением Правительства – Постановление от 18.09.2012 № 940. Хотя о том, что могут объединения операторов потуже затянуть веревку на шее своих членов и «развести» их на дополнительные деньги на нейтрализацию дополнительных угроз, постановление, естественно, молчит. Как и о том, почему в организациях и учреждениях одного из министерств до недавнего времени можно было защищать персональные данные специальных категорий по минимальным требованиям, не соответствующим последствиям неправомерного доступа к ним.

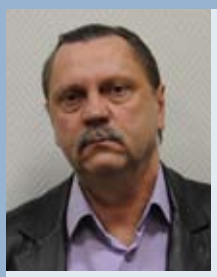
Поэтому модель поведения операторов в условиях принятых на сегодняшний день требований, не устанавливающих обязательных случаев защиты от угроз, связанных с недекларируемыми возможностями системного и прикладного программного обеспечения, просматривается совершенно очевидная – признать актуальными только угрозы третьего типа (не связанные с использованием злоумышленником тех самых недокументированных возможностей) и защищаться по минимальным требованиям.

При этом надо отметить два важных момента.

По закону и в соответствии с Постановлением Правительства № 1119 оценка вреда, определение актуальных типов угроз и актуализация их модели – прерогатива оператора, а не регулятора или надзорного органа. В то же время в соответствии с ч. 5 ст. 19 Федерального закона «О персональных данных» угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки, определяют федеральные органы исполнительной власти, выполняющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий. И коль скоро появятся новые документы, обязывающие операторов, занимающихся определенными видами деятельности, считать актуальными угрозами наличие недекларируемых возможностей в используемом ими софте, такое решение при возникновении излишествующих обременений для операторов можно оспорить и в суде.

И второе. Если оператор рискнет признать актуальными угрозы, связанные с недокументированными возможностями программного обеспечения, ему придется за свой счет и на собственный страх и риск выполнить работу по оценке исходного кода, заключив договор с организацией, готовой такие угрозы оценить. Потому как требований по отсутствию недокументированных возможностей для операционных систем и приложений в нашей стране нет, они сформулированы только для средств защиты информации, и никакой ответственности за полученные результаты организация, выполнившая анализ исходного кода, по закону не несет. Да и не понятно пока, кто подтвердит корректность и полноту произведенных оценок – систем сертификации для этих проблем, ни добровольных, ни обязательных, пока тоже нет. Оценка соответствия полученных результатов чему бы то ни было повисает в воздухе.

мнение специалиста



Владимир ГУСЬКОВ,
руководитель отдела технической поддержки, компания SafenSoft

Анализ категорий операторов, осуществляющих обработку персональных данных, на действия которых чаще всего поступают жалобы от персональных пользователей, позволяет утверждать, что лидерами хищения персональных данных являются: кредитные учреждения, жилищно-коммунальные организации, операторы связи и страховые компании.

Из перечисленных выше категорий операторов по обработке персональных данных только три используют для оплаты устройства самообслуживания (терминалы), в которых обрабатывается такая информация: ФИО, место жительства, телефоны, номера счетов, что подпадает под закон о защите персональных данных. Таким образом, появилась необходимость как физической, так и системной защиты самих устройств самообслуживания.

Так как терминалами чаще всего владеют кредитные учреждения (банки), то они должны позаботиться о защите терминалов на программном уровне, что на данный момент исполняется не всеми. Такая защита должна соответствовать всем требованиям банковских стандартов по защите конфиденциальных данных, а значит, и системы, на которых обрабатываются персональные данные, должны быть защищены специальным программным обеспечением, обладающим всеми необходимыми сертификатами и лицензиями. На данный момент появляется новое специализированное программное обеспечение, которое не позволяет сторонним пользователям, не имеющим права доступа к персональным данным, а также администраторам удалять, изменять и копировать эти данные.

Операторы, не соблюдающие требования Закона «О защите персональных данных», должны наказываться.